



**Pasi Yliluoma**  
Toimitusjohtaja  
Ymon Oy

# Tietoturva on osa johtamista

**T**ietoturva ei ole rakettitiedettä. Se on tapa toimia oikein kaikessa päivittäisessä työssä. Tietoturva on pääosin varmistettavissa maalaisjärjellä ja pitkäjänteisellä työllä. Tärkeintä on, että johtaja puhuu tietoverkoista ja tietoturvasta kuten niistä pitää puhua: liiketoiminnan kielellä. Kun noudatat seuraavia käskyjä, tietoturvaan liittyvät turhat pelot katoavat ja nukut yösi hyvin.

## 1 Näytä esimerkkiä

Usein johto vaatii henkilöstöä noudattamaan tietoturvasääntöjä ja muita ohjeita kuvitellen, että ohjeet eivät koske meitä.

Kyllä koskevat. Vain näyttämällä itse hyvää esimerkkiä opetat muutkin toimimaan oikein.

## 2 Tee selkeä vastuutus

Päätä, kuka johtaa yrityksesi tietoturva- ja riskienhallintatoimintaa. Suurissa yrityksissä tarvitaan riskienhallintajohtaja, pienissäkin tietoturvapääällikkö. Ota hänet mukaan johtoryhmään, anna valta ja vastuu. Vaadi häneltä säännöllinen raportointi liiketoiminnan ehdoilla ja kielellä.

## 3 Suojaa aineeton omaisuus

Monessa yrityksessä kiinteistön ja kaluston vakuutukset ovat kunnossa, mutta ihme kyllä yrityksen aineeton omaisuus kuten tietokannoissa oleva tieto, on suojaamatta. Tämä on järjetöntä, sillä yritysten tietoverkoissa makaa yleensä enemmän kriittistä pääomaa kuin esimerkiksi kiinteistöissä.

Budjetoi aineettoman omaisuuden suojaamiseen riittävästi rahaa. Tietoturvan vastuuhenkilö varmasti etsii tarvittavat tekniset suojavälineet.

## 4 Anna riittävät resurssit

Noin 25 vuoden kokemukseni mukaan yhdeksässä tapauksessa kymmenestä yrityksen tietoverkko on erilainen kuin sen luullaan olevan. Sitä paitsi se toimii eri tavalla kuin sen on tarkoitettu toimivan.

Jotta tietoverkko tukee liiketoimintaa, siihen on satsattava rahaa ja henkilöstöä. Kaikkea ei tarvitse tehdä itse, vaan alan ammattilaisille kannattaa maksaa puolueettomasta suunnittelusta.

Kun tietoverkko ja sen tietoturva on suunniteltu hyvin, voit reagoida ennalta etkä vasta sitten, kun yritykseen tulee tietomurto. Tiedä verkkosi, sen toiminta ja ketkä sitä käyttävät. Tavoitteena kannattaa olla tietoverkko, joka vastaa asiakkaidesi, kumppanisi ja työntekijöidesi vaateita.

## 5 Tarkkaile poikkeamia

Tietoverkko elää ja muuttuu jatkuvasti. Siksi tietoverkon toimintaa on seurattava jatkuvasti.

Kannattaa miettiä ja asettaa tietoverkon toiminnalle ja tietoturva-asioille yksinkertaiset hälytysrajat. Jos

hälytysraja ylittyy, tietotekniikkaväen on syytä reagoida heti poikkeamiin.

## 6 Tee ohjeista todellisuutta

Hyvästikään ohjeista ei ole hyötyä kassakaapissa. Anna työntekijöidesi vaikuttaa ohjeiden sisältöön. Näin sitoutat heidät parhaiten noudattamaan ohjeita. Jaa ohjeet koko henkilöstölle, puhu niistä ja kehota esimiehiä näyttämään porukalleen esimerkkiä.

## 7 Analysoi sisäiset uhkat

Yli 80 prosenttia tietoturvaongelmista lähtee yrityksen sisältä. Analysoi yrityksesi sisäiset tietoturva-uhkat ja toimi tämän mukaan.

Laki asettaa vaateita esimerkiksi sille, kenellä on oikeus sisäpiiriin tietoon. Eikä Salainen-Julkinen ole riittävä luokittelu tietoverkossa liikkuville tiedoille.

## 8 Analysoi ulkoiset uhkat

Lähes kaikissa yrityksissä on kulunvalvonta ja tallentavat videokamerat fyysisen turvallisuuden varmistamiseen. Mutta miten on tietoverkkojen laita?

Tietojärjestelmien ja tietoverkkojen valvonta- ja murtohälytysjärjestelmä täytyy suunnitella ja toteuttaa riskien vaatimalle tasolle.

## 9 Hyödynnä uusia mahdollisuuksia

Saat aikaan suuria säästöjä ja tehostat toimintaa, kun hyödynnät esimerkiksi tietoverkon virtualisointia, ulkoistamista ja pilvipalveluja. Ne ovat hyvin suunniteltuina täysin turvallisia, mutta väärin tehtyinä vaarantavat tietoturvan.

Luotettavien it-kumppanien valintaan kannattaa käyttää aikaa. Vaadi ja valvo, että kumppanisi noudattavat ohjeita.

## 10 Muista aina ihminen

Media kertoo tämän tästä henkilö- ja pankkikorttitietojen varkauksia. Tietoturvarikoksia tekevät ihmiset - eivät koneet! Nykyään tietoturvarikos on usein kansainvälinen, sillä rikollisia eivät pidättele maiden rajat eivätkä lait.

**Henkilöstösi käyttää tietoverkkoa** työssään päivittäin. Ihminen on aina tietoturvan heikoin lenkki. Koulu- ja organisaatiosi, niin se voi toimia fiksusti verkossa ja kärkeä epävakaat asiat, ennen kuin ne saavat aikaan korvaamatonta tuhoa.

Kun teet tietoturvasta henkilöstöllesi tärkeän asian, henkilöstö on vahva voimavarasi.

**Tietoverkoissa makaa enemmän kriittistä pääomaa kuin kiinteistöissä.**

Väitä vastaan: [talouselama.fi/minavaitan](http://talouselama.fi/minavaitan)